



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/773,187	01/31/2001	John Steven Langford	AUS920000943US1	4502
45993	7590	04/25/2005		
IBM CORPORATION (RHF) C/O ROBERT H. FRANTZ P. O. BOX 23324 OKLAHOMA CITY, OK 73123			EXAMINER DADA, BEEMNET W	
			ART UNIT 2135	PAPER NUMBER

DATE MAILED: 04/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/773,187	<b>Applicant(s)</b> LANGFORD ET AL.	
	<b>Examiner</b> Beemnet W Dada	<b>Art Unit</b> 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 04 October 2004.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-16 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

A

## **DETAILED ACTION**

1. This office action is in reply to an amendment filed on October 04, 2004. Claims 1-16 are pending.

### ***Response to Arguments***

2. Applicant's arguments, filed on October 04, 2004 with respect to the rejection(s) of claim(s) 1, 6 and 11 under 35 USC 102(e) in view of Crosbie et al. (US Provisional Application 60/210,922) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Crosbie et al. US Publication 2002/0083343 A1, which claims priority under 35 U.S.C 119(e) to U.S. Provisional application 60/210,922, having an earlier effective U.S. filing date which is relied on to reject the claims in the present application (See MPEP § 2136.02 and MPEP § 2136.03 III).

### ***Claim Rejections - 35 USC § 102***

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Crosbie et al. US Publication 2002/0083343 A1 (hereinafter Crosbie) [US Publication 2002/0083343 A1 claims priority under 35 U.S.C 119(e) to U.S. Provisional application 60/210,922, having an earlier effective U.S. filing date which is relied on to reject the claims in the present application (See MPEP § 2136.02 and MPEP § 2136.03 III)].

5. As per claims 1, 6 and 11, Crosbie teaches a method for detecting possible security violations and issues in a computer system related to user ID substituting and switching (i.e., 'SU' ing), said computer system having a log of user ID substitutions and switches, said method comprising the steps of:

providing a set of rules which define conditions of user ID substitutions and switches which are to be considered possible security issues (i.e., repeated number of SU attempts within a certain period of time) [page 14, paragraphs 0345-0353, page 9, paragraph 0195];

providing a process adapted to evaluate said log of user ID substitutions and switches according to said set of rules (i.e., monitoring and analyzing su log information to detect security violations) [page 14, paragraphs 0345-0347, page, 11, paragraph 0225 and page 6, paragraphs 0114-0115];

evaluating said log of user ID substitutions and switches to find any entries in said log which meet one or more defined conditions in said set of rules (i.e., monitoring and analyzing su log information to detect security violations) [page 14, paragraphs 0345-0347, page 13, paragraphs 0301-0308 and page 6, paragraphs 0114-0115]; and

outputting an alert responsive to finding one or more log entries which meet said conditions [page 21, paragraph 0756-0757 and page 7, paragraphs 0131-0134].

6. As per claims 4, 9 and 15, Crosbie teaches the method as applied above. Furthermore, Crosbie teaches, the method, wherein said step of evaluating said log of user ID substitutions and switches comprises evaluating a SLOG file in a system having a UNIX-like operating system (i.e. HP-UX system) [page 4, paragraph 0067].

7. As per claims 5, 10, 16, Crosbie teaches the method as applied above. Furthermore, Crosbie teaches, the method, wherein said step of outputting an alert comprises sending an electronic message to a predetermined destination address [page 21, paragraph 0756-0757 and page 7, paragraphs 0131-0134].

8. As per claims 2, 3, 7, 8, and 12-14 Crosbie teaches evaluating log of user ID substitutions and switches to find any entries in said log which meet one or more defined conditions in said set of rules (i.e., monitoring and analyzing su log information to detect security violations) [page 14, paragraphs 0345-0347, page, 11, paragraph 0225 and page 6, paragraphs 0114-0115], in a UNIX-like operating system (i.e. HP-UX system) [page 4, paragraph 0067], and further teaches evaluating a log with a simple daemon (which meets the recitation) [column 8, paragraph 0156-0159].

### ***Conclusion***


9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

April 11, 2005



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100